

REMARKS

Applicant respectfully requests consideration and allowance of the pending claims. Claims 1, 8 and 15 are independent, and the same claims are amended hereby.

Double Patenting

Claims 1-20 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6, 8-18, 20-29, 31-40 and 42-47 associated with U.S. Patent Application No. 10/609,260. The Office has agreed to hold the rejection in abeyance until allowable subject matter is identified.

Claim Rejections Under 35 U.S.C. § 112

Claims 1-20 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Applicant respectfully traverses the rejection.

The basis of this rejection stems from the added subject matter: "*said blind digital signature corresponding to a single element in said Jacobian of said at least one curve.*" See, for example, claim 1. Applicant has amended the indicated subject matter to further clarify the subject matter. For example, claim 1 now recites the subject matter: "*said blind digital signature having a length corresponding to a single element in said Jacobian of said at least one curve.*" The subject matter of claims 8 and 15 has been amended in a similar manner.

Support for the amended subject matter is found in, for example, paragraph [0113] of the instant Application. This paragraph is preceded by a detailed

explanation of Jacobians in connection with curves. Review of the indicated portion of the instant Application shows that the claims of the instant Applicant comply with 35 U.S.C. § 112, first paragraph. Accordingly, the Office is respectfully requested to withdraw the rejection.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-20 stand rejected as being unpatentable under 35 U.S.C. § 103(a) in view of a publication to Boldyreva ("Efficient Threshold Signature, Multisignature Schemes Based On The Gap-Diffie-Hellman-Group Signature Scheme") and Zhang et al. ("ID-Based Blind Signature and The Rating Signature from Pairings") ("Zhang"). Applicant respectfully traverses this rejection.

Applicant addresses the rejection of the independent claims in the following. As a preliminary matter, Applicant does not separately address the patentability of each remaining dependent claim in detail. However, Applicant's decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that Applicant concurs with the Office's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, Applicant's decision not to discuss differences between the prior art and every claim element, or every comment made by the Office, should not be considered as an admission that Applicant concurs with the Office's interpretation and assertions regarding those claims. Indeed, Applicant believes that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least

the same reasons as the independent claims from which the dependent claims ultimately depend.

Amended Claim 1 recites:

A method comprising:
receiving first data to be blindly signed;
establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of at least one curve, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;
determining private key data and corresponding public key data using said signature generating logic;
generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature, *said blind digital signature having a length corresponding to a single element in said Jacobian of said at least one curve*; and
disseminating the second data to a computing device. (Emphasis added.)

Respectfully, none of the references, alone or in combination, suggests what is recited by **claim 1** for at least the following reasons.

As those of ordinary skill in the art appreciate, current digital signature schemes, such as those based on conventional Computational Diffie-Hellman assumptions, produce relatively long digital signatures in an attempt to improve security. However, such long digital signatures are not generally user friendly.

Coupled with the novel use of a Jacobian of at least one curve, a "blind digital signature *having a length corresponding to a single element* in said Jacobian of said at least one curve" may be generated from the novel limitations recited by claims 1, 8 and 15. Using the Jacobian of at least one curve enables the use of a much simplified blind digital signature (e.g., a blind digital signature that has a length that corresponds to a signal element in the Jacobian).

Boldyreva discloses a conventional blind signature scheme based on the use of the conventional Gap Diffie-Hellman (GDH) group. The blind signature scheme is discussed in detail in Section 6, page 12, of the Boldyreva document. The description of the indicated Section clearly shows that Boldyreva does not suggest producing a blind digital signature that has "a length" that corresponds to a "single element" in a "Jacobian of at least one curve."

The Office has relied upon Zhang to show that GDH groups may be derived from a Jacobian of a curve. The Office points to page 7, first paragraph, of the Zhang publication. In this paragraph Zhang discloses that the signature consists of an element in G and an element in V . G is a cyclic group generated by P , whose order is a prime q , and V is a cyclic multiplicative group of the same order q . (See page 3, second paragraph, of Zhang.)

However, Zhang does not suggest that the size of the signature corresponds to a "single element" in a Jacobian of a curve. Instead, Zhang discloses that the signature consists of the elements G and V . Zhang then discloses that the size of element G can be reduced by compression. Therefore, *first* Zhang discusses what the signature includes, and *second* discusses the size of an element in the signature. However, Zhang does not describe the size of the signature.

Therefore, even if one of ordinary skill in the art were to combine the teachings of the Zhang with those of Boldyreva, which the Applicant does not concede, the combination does not suggest at least producing a "blind digital signature having a length corresponding to a single element in said Jacobian of said at least one curve." (Claim 1.)

According to the foregoing, Applicant respectfully submits that the combination of Boldyreva in view of Zhang does not suggest the limitations of claim 1.

Applicant will now address the rejections of **claims 8 and 15**. For brevity, claims 8 and 15 are not reproduced in their entirety below.

The combination of Boldyreva in view of Zhang fails to suggest what is recited in claim 8. For example, the combination fails to disclose or suggest at least "said blind digital signature having a length corresponding to a single element in said Jacobian of said at least one curve." (Claim 8.) A discussion of the deficiencies of the combination in connection with at least this limitation of claim 8 is given above. Applicant submits that other limitations of this claim may also show that the recitation of the claim is novel and non-obvious.

The combination of Boldyreva in view of Zhang fails to suggest what is recited in claim 15. For example, the combination fails to disclose or suggest at least "said blind digital signature having a length corresponding to a single element in said Jacobian of said at least one curve." (Claim 15.) A discussion of the deficiencies of the combination in connection with at least this limitation of claim 15 is given above. Applicant submits that other limitations of this claim may also show that the recitation of the claim is novel and non-obvious.

Claims 2-7, 9-14 and 16-20 are at least allowable due to their dependency upon an allowable independent claim, as well as for additional limitations set forth by the claims.

The detailed discussion above shows that Boldyreva and Zhang, whether taken alone or in combination together, fail to suggest the claims rejected under 35 U.S.C. § 103(a). Accordingly, reconsideration and withdrawal of the rejection are respectfully requested.

Conclusion

In accordance with the foregoing remarks, Applicant believes that the pending claims are allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the Applicant at the telephone number provided below.

Respectfully Submitted,

Dated: December 21, 2007

By: David L. L. Reg. No: 38,222
for Tim R. Wyckoff
Reg. No. 46,175
206-315-4001